IBM Security QRadar
Versión 7.2.6

Guía de consulta rápida de Packet Capture

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado "Avisos" en la página 7.

Información sobre el producto

Este documento corresponde a IBM QRadar Security Intelligence Platform V7.2.6 y a todos los releases subsiguientes a menos sea reemplazado por una versión actualizada de este documento.

Contenido

Acerca de esta guía de consulta rápida de Packet Capture

Esta documentación le proporciona la información de consulta rápida que necesita para instalar y configurar IBM® Security QRadar Packet Capture. QRadar Packet Capture está soportado por IBM Security QRadar SIEM.

Público al que se dirige

Los administradores del sistema responsables de la instalación de QRadar Packet Capture deben estar familiarizados con los conceptos de seguridad de red y las configuraciones de dispositivos.

Documentación técnica

Para buscar documentación del producto IBM Security QRadar en la biblioteca de productos de QRadar, consulte Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Cómo ponerse en contacto con el servicio de soporte al cliente

Para obtener información acerca de cómo ponerse en contacto con el servicio de soporte al cliente, consulte la nota técnica sobre soporte y descarga (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Declaración de buenas prácticas de seguridad

La seguridad de los sistemas de TI implica la protección de sistemas e información mediante la prevención, la detección y la respuesta a accesos indebidos desde dentro o fuera de la empresa. Un acceso indebido puede alterar, destruir o dar un uso inapropiado de la información o puede ocasionar daños o un uso erróneo de sus sistemas, incluidos los ataques a terceros. Ningún producto ni sistema de TI debe considerarse completamente seguro, y ningún producto, servicio o medida de seguridad por sí solo debe considerarse totalmente eficaz para evitar el acceso o el uso indebidos. Los sistemas, productos y servicios de IBM están diseñados como parte de un procedimiento global de seguridad de acuerdo con la legalidad vigente, lo que implica necesariamente procedimientos operativos adicionales, y pueden requerir otros sistemas, productos o servicios para ser más eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, O HAGAN QUE SU EMPRESA SEA INMUNE, A LAS CONDUCTAS MALICIOSAS O ILEGALES DE TERCEROS.

Tenga en cuenta lo siguiente:

El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM Security QRadar solamente se puede utilizar con fines legales y de forma legal. El cliente se compromete a utilizar este Programa de acuerdo con las leyes, disposiciones y políticas aplicables, y asume toda la responsabilidad de su cumplimiento. El licenciatario declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM Security QRadar.

Capítulo 1. Actualización de QRadar Packet Capture

Para actualizar de QRadar Packet Capture V7.2.5 a V7.2.6, instale un fixpack de software acumulativo en una aplicación de QRadar Packet Capture. La versión de software que está instalada en la aplicación debe ser la compilación 7.2.5.230.

Procedimiento

1. Asegúrese de que no hay captura de paquetes ni actividades de búsqueda en curso.
2. Utilice SSH para iniciar la sesión en el sistema como usuario `root`.
3. Descargue el fixpack `7.2.6-QRadar-PCAP-build-238.sfs` de IBM Fix Central (http://www.ibm.com/support/fixcentral/)
4. Copie el fixpack en el directorio `/tmp`.

   Si el espacio en el directorio `/tmp` es limitado, copie el fixpack en otra ubicación que tenga espacio suficiente.
5. Cree el directorio `/updates` tecleando el mandato siguiente:

   ```
   mkdir -p /updates
   ```
6. Utilice el mandato **cd** para situarse en el directorio en el que ha copiado el archivo de fixpack.

   ```
   cd /tmp
   ```
7. Para montar el archivo de fixpack en el directorio `updates`, teclee el mandato siguiente:

   ```
   mount -o loop -t squashfs 7.2.6-QRadar-PCAP-build-238.sfs /updates
   ```
8. Para ejecutar el instalador para el fixpack, cambie el directorio al directorio `/updates` y teclee el mandato siguiente:

   ```
   sh installer.sh
   ```
9. Reinicie el sistema.

Capítulo 2. Guía de consulta rápida de QRadar Packet Capture

Para poder capturar paquetes, debe configurar valores de red y de conexión de IBM Security QRadar Packet Capture.

Lista de compatibilidad de Intel SFP+ y SFP

El dispositivo de QRadar Packet Capture solo tiene un puerto de captura (DNA0). El dispositivo de QRadar Packet Capture no está equipado con un transceptor de conectable de formato pequeño por lo que debe instalar un SFP+ 10G o un SFP 1G (RJ45 de cobre) en el puerto de captura.

Para adquirir un transceptor de 10G, consulte la página web de Digi-Key (http://www.digikey.com/product-detail/en/FTLX8571D3BCL/775-1060-ND/1967719?WT.srch=1&WT.medium=cpc&WT.mc_id=IQ66882673-VQ2-g-VQ6-45013742355-VQ15-1t1-VQ16-c).

Para adquirir un transceptor de 1G, consulte la página web de Digi-Key(http://www.digikey.com/product-detail/en/FCLF-8521-3/775-1003-ND/1832807)

Una vez instalado el SFP 1G, trunca la tasa de captura a 1 Gbps.

Para tener varias conexiones de 1G, puede poner un conmutador o un agregador delante de donde el puerto de salida de 10G entra en el puerto de SFP+ 10G de QRadar Packet Capture. Como resultado, tendrá varios puertos de 1Gb agregados en la interfaz de 10G SFP+ de QRadar Packet Capture.

La lista siguiente muestra los requisitos de módulo SFP+ y SFP:

Número de pieza	**Descripción**
E10GSFPSR	10GBASE-SR/1000BASE-SX de tasa dual, Intel Ethernet SFP+ SR óptico
E10GSFPLR	10GBASE-LR/1000BASE-LX de tasa dual, Intel Ethernet SFP+ LR óptico
ABCU-5710RZ	1000BASE-T, Transceptor Gigabit Ethernet de Avago
FCLF8522P2BTL	1000BASE-T, Transceptor Gigabit Ethernet de Finisar
453153-001	Transceptor Gigabit SX de HP

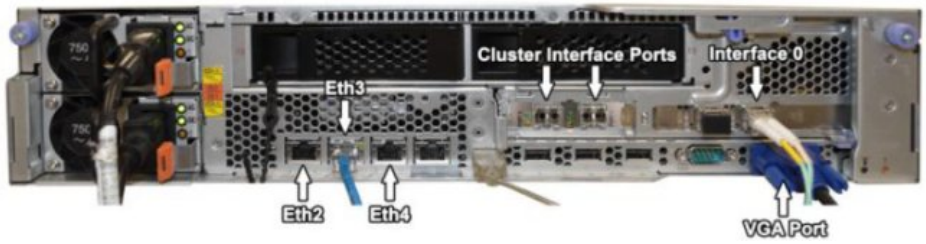
Configuración de red

Para configurar inicialmente la red, son necesarios un monitor, un teclado y una conexión Ethernet a un puerto interno. De forma predeterminada, el sistema tiene puertos DHCP activos.

Si sabe la dirección IP del puerto Ethernet que se está utilizando, vaya a Iniciar grabación.

1. Proporcione una conexión de red para el acceso remoto al servidor.

   Proporcione una conexión Ethernet a uno de los puertos Ethernet integrados eth2, eth3 o eth4, tal que se muestra en el diagrama siguiente.



2. Proporcione una conexión de red para la captura de red.

   Proporcione conexiones de fibra 10G mediante los puertos de interfaz 0 que se muestran en el diagrama siguiente.

   Importante: Asegúrese de que haya tráfico por las conexiones. Para capturar tráfico, debe utilizar un puerto Tap o SPAN (duplicado). Cuando utiliza un puerto SPAN en un conmutador, si el conmutador asigna una prioridad menor al puerto SPAN, se podrían eliminar algunos paquetes.

3. Utilice SSH para iniciar la sesión.

   Después de iniciar el sistema, inicie una sesión utilizando la información de usuario siguiente:

   Usuario: `continuum`

   Contraseña: `P@ck3t08..`

4. Registre la dirección IP.

   Después de iniciar una sesión, abra un terminal y emita el mandato siguiente: `#ifconfig -a`

   Este mandato proporciona la dirección IP del puerto Ethernet que está conectado.

   Nota: Para obtener información acerca del establecimiento de una dirección IP estática, consulte la publicación *Guía del usuario de IBM Security QRadar Packet Capture*.

5. Pruebe la conexión.

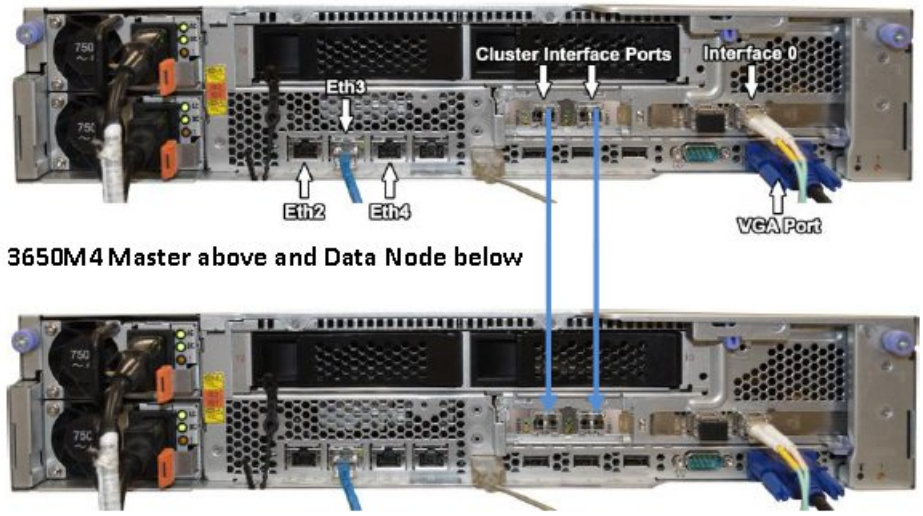
   Para probar la conexión, ejecute un mandato ping para la red interna o inicie una sesión remota mediante SSH en el puerto 4477. Asegúrese de que haya una conexión satisfactoria antes de continuar.

Conecte el clúster

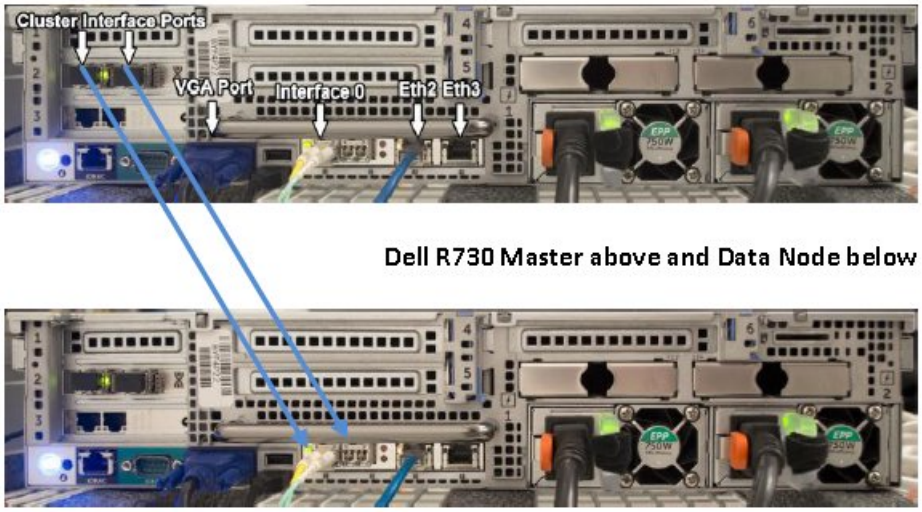
Una vez que haya conectado satisfactoriamente la red al sistema autónomo o maestro, conecte el dispositivo de captura de paquetes maestro a los dispositivos

de Nodo de datos de QRadar Packet Capture. Si solo tiene un sistema de captura de paquetes autónomo, este paso no es necesario.

1. Consulte el diagrama de hardware para el dispositivo de captura de paquetes.
   - Conexión del dispositivo de captura de paquetes maestro IBM System x3650 M4 y el Nodo de datos de QRadar Packet Capture



   - Dispositivo de captura de paquetes Dell R730 y Nodo de datos de QRadar Packet Capture



2. En la parte posterior del dispositivo de captura de paquetes, conecte el puerto de interfaz de clúster de la izquierda del maestro con el puerto de interfaz de clúster de la izquierda del primer nodo de datos, tal como indican las flechas de los diagramas precedentes.
3. Si hay un segundo nodo de datos, conecte el puerto de interfaz de clúster de la derecha del maestro con el puerto de interfaz de la derecha del segundo nodo de datos.
4. En un terminal del sistema maestro, compruebe las conexiones con una prueba ping:

```
ping 1.1.1.2
ping 2.2.2.2
```

5. Si no recibe una respuesta de ping, intercambie las conexiones de cable solo en las interfaces de nodo de datos.
   - Si solo se conecta un nodo de datos, solo un ping debe responder satisfactoriamente.
   - Si después de conectar los cables sigue sin haber respuesta de la prueba ping, pase los cables de la tarjeta de interfaz de red del nodo de datos a la segunda tarjeta de interfaz de red Ethernet óptica instalada (si hay una) y repita la prueba ping.

Iniciar el registro

Una vez que haya una conexión de red satisfactoria con el sistema, puede empezar a registrar paquetes de red en disco y ver estadísticas sobre el tráfico de una red.

1. Inicie la interfaz web.

   En cualquier sistema remoto que esté conectado a la red, abra un navegador web y escriba la dirección IP seguida de `/login.html`.

   Ejemplo: `http://192.168.1.1/login.html`
2. Inicie una sesión.

   Se abre la pantalla de inicio de sesión de QRadar Packet Capture.

   Se crea una cuenta predeterminada.

   Escriba el nombre de usuario y la contraseña siguientes:

   `Usuario`: `continuum`

   `Contraseña`: `P@ck3t08..`

   La primera vez que inicie la sesión se le pedirá que cambie la contraseña.
3. Habilite cada nodo de datos (slave) que ha conectado físicamente.
4. Inicie el registro.

   Una vez que haya iniciado la sesión y habilitado los nodos de datos, vaya a la página **Estado de captura** y pulse **Iniciar captura**.

   Nota: Cuando la captura comienza, se muestra una ventana de estadísticas que contiene todos los detalles de la captura.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implicar que solo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen la materia descrita en este documento. La posesión de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785, EE. UU.

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japón

El párrafo siguiente no es aplicable en el Reino Unido ni en ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícita ni explícita, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no sea aplicable en su caso.

Esta información podría incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias hechas en esta publicación a sitios web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de estos sitios web. El contenido de esos sitios web no forma parte del contenido de este producto de IBM, por lo que la utilización de dichos sitios es responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir:(i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se haya intercambiado, deberán ponerse en contacto con:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, EE. UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluyendo, en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del contrato de cliente IBM, el contrato internacional de licencia de programa de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas en nivel de desarrollo y no existe garantía alguna de que estas mediciones sean iguales en los sistemas de disponibilidad general. Además, es posible que algunas mediciones se hayan calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, compatibilidad o cualquier otra declaración relacionada con los productos que no son de IBM. Las preguntas relativas a las prestaciones de los productos que no son de IBM deberán dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la orientación o intención futura de IBM están sujetas a cambio o anulación sin previo aviso y representan solamente metas y objetivos.

Todos los precios de IBM mostrados son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales cotidianas. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos

esos nombres son ficticios y cualquier similitud con los nombres y direcciones utilizados por empresas reales es mera coincidencia.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de www.ibm.com/legal/copytrade.shtml.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de terceros.

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software que se ofrece como soluciones de servicio (Ofertas de software), pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, ayudar a mejorar la experiencia del usuario final, ajustar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se define información sobre el uso de cookies de esta oferta.

En función de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que recopilan el ID de sesión de cada usuario para la gestión y autenticación de sesiones. Estas cookies se pueden inhabilitar, pero si se inhabilitan también se elimina la función que estas cookies habilitan.

Si las configuraciones desplegadas para esta oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, que incluye cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de diversas tecnologías, incluidos los cookies, para estos fines, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, la sección titulada “Cookies, Web Beacons and Other Technologies” y la declaración “IBM Software Products and Software-as-a-Service Privacy Statement” en http://www.ibm.com/software/info/product-privacy.